A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL (617) 727-6200

No. 2001-0054-4F

OFFICE OF THE STATE AUDITOR'S
REPORT ON INFORMATION TECHNOLOGY AND FINANCIAL-RELATED CONTROLS
AT THE MASSACHUSETTS REHABILITATION COMMISSION

July 1, 2000 through April 24, 2001

OFFICIAL AUDIT REPORT

SEPTEMBER 28, 2001

2001-0054-4F

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts Rehabilitation Commission (MRC) is authorized under Chapter 6, Section 7A, of the Massachusetts General Laws, and is placed under the Executive Office of Health and Human Services. The Commission is staffed by approximately 740 employees under the direction of a full-time Commissioner of Rehabilitation. Three hundred and forty of the Commission's employees are direct-service counselors. Oversight and guidance are provided by an Advisory Council of fourteen members who serve without compensation. The MRC operates from one administrative office, twenty-seven area offices, and five district offices located in various cities and towns throughout the Commonwealth.

The MRC's primary mission is to provide its clients with an array of comprehensive services that help to maximize their quality of life and enable them to become economically self-sufficient. Specific programs to assist the MRC's clients include, but are not limited to, the Disability Employment Project (DEP), Independent Living Project (ILP), Rehabilitation Services (RS), Support Housing Program (SHP), Minorities Disabilities Support Program (MDSP), Personal Care Assistance (PCA), and a state-wide Head Injury Program.

The MRC uses information technology (IT) and systems to support the mission of the agency. At the time of our audit, MRC's IT infrastructure included six file servers installed at the Commission's administrative office, approximately 1,100 microcomputers, configured in a Microsoft NT local area network (LAN), and 100 laptop computers available to support field and office operations of MRC's wide area network (WAN). LANs are installed at area and district offices and are being used for office operations and access to printing client-related and other business documents. Through the Commonwealth's WAN, each area and district office can gain access to the Commission's Client Tracking System and the Massachusetts Management Accounting and Reporting System (MMARS). Both of these systems are operated on the Commonwealth's Information Technology Division's (ITD) IBM mainframe located at the Massachusetts Information Technology Center. The MRC's UNIX-based file server, which provides access to the state's WAN, also enables communication with other state agencies and the Internet.

The Commission plans to fully migrate its Client Tracking System by December 2001 from ITD's IBM mainframe to an MRC-operated LAN-based case management system. At the time of our audit, the Client Tracking System, which is known as the Massachusetts Rehabilitation Commission Information System (MRCIS), was being parallel tested on an Oracle database.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From January 8, 2001 through April 24, 2001, we conducted a follow-up audit at the Massachusetts Rehabilitation Commission (MRC) for the period of July 1, 2000 through April 24, 2001. The audit consisted of a follow-up examination of selected information technology (IT) and financial-related internal control areas brought forward from our prior audit report (No. 96-0054-4C), issued July 16, 1997. The scope of the audit consisted of an examination of hardware and software inventory control, authorized use of software, logical access security, and business continuity planning. Our review of business continuity planning included an evaluation of on-site and off-site storage of computer-related backup media.

In addition to our review of prior audit results, we examined controls regarding the safeguarding and disposal of confidential records and access security over the client database.

Audit Objectives

The primary objective of our audit was to determine whether corrective action had been taken regarding audit results and recommendations brought forward in our prior IT audit report. We determined whether adequate controls were in place and in effect for the selected IT and financial-related areas.

We sought to determine whether controls were in place to prevent and detect the existence of unauthorized and/or illegal copies of licensed software on Commission computers. We sought to determine whether adequate business continuity plans were in place to ensure that IT functions could be regained within an acceptable period of time should a disaster render the Commission's IT systems inoperable or unavailable. We also sought to determine whether adequate media backup procedures were being performed and whether copies of mission-critical and essential IT-related magnetic media were stored in secure on-site and off-site locations. In addition, we sought to determine whether access to the LAN file servers and microcomputer systems was adequately restricted to authorized users in order to prevent damage to, or loss of, computer equipment or IT-related media. We also sought to determine whether sufficient inventory controls were in effect to properly account for hardware and software.

Our objectives with respect to the financial-related areas were to assess controls regarding the IT-related asset inventory and compliance with Generally Accepted Accounting Principles (GAAP) for reporting requirements and to assess the associated internal control environment. Specifically, our follow-up review of financial-related controls concerned the adequacy of fixed-asset inventory procedures and the relevance and reliability of inventory records for IT resources. We evaluated

whether adequate inventory controls were in place to provide reasonable assurance that IT equipment and software were properly accounted for and safeguarded against unauthorized use, theft, or damage. An additional objective was to ascertain whether MRC was properly safeguarding and disposing of confidential client data and hardcopy documents.

Audit Methodology

To determine whether the audit should address each of the prior audit results, or any other areas, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations and relevant internal controls through interviews, observation, and documentation review. In conjunction with our review of the internal control environment, we determined whether the MRC had developed and implemented written, authorized, and approved internal control documentation including IT-related policies and procedures, and assessed the adequacy of the documentation with respect to control objectives related to our audit. To accomplish a preliminary review of the adequacy of general controls over IT-related assets, we obtained an understanding of IT operations at the MRC, inspected locations within the MRC administrative office housing the LAN file servers and the microcomputer systems, and performed an overall risk analysis of IT operations and related areas. To assess the adequacy of IT-related general controls, we used audit checklists and audit guides; interviewed management, administrative and technical staff, and microcomputer users; observed operations; and performed selected audit tests.

To determine whether adequate inventory controls were in place over hardware and software, we determined whether the Commission maintained a record of inventory for fixed assets or a separate inventory for hardware and software. With respect to the inventory record of hardware and software, we determined whether appropriate fields of information were included. To assess the accuracy and completeness of the inventory record, we compared a random sample of fixed-asset items to the Commission’s inventory record. We reviewed software residing on microcomputers and laptop computers to determine whether management had authorized and approved the use of software and whether software packages and products were listed on the inventory record.

To determine whether adequate controls were in place to prevent unauthorized access to the Commission’s automated systems, we reviewed physical security over IT resources and logical access security to the automated systems. Our review included an assessment of documented policies and procedures regarding physical and logical security and security administration, procedures for activating and deactivating system users, and password administration.

We determined whether the MRC's logical access security policies and procedures prevented and detected unauthorized access to the data files and software installed on the LAN file servers, microcomputer systems, and laptop computers. Our tests of logical access security included a

review of access privileges for those staff who were authorized to access the LAN file servers, microcomputer systems, and laptop computers located at MRC offices. Subsequently, we determined whether all staff authorized to access the automated systems were required to change their passwords periodically and the frequency of the changes.

To determine whether the administration of logon ID and password security was being properly carried out, we reviewed security procedures with the MRC's Security Administrator responsible for access to the LAN file servers, microcomputer systems, and laptop computers. Because the Client Tracking System, which is the repository of the MRC's most critical and important data, resides on the IBM mainframe in Chelsea at the Information Technology Center, we determined whether adequate controls were in place to ensure that access privileges were granted to only authorized users. Also, since a test version of the Client Tracking System was in development in an Oracle database, we reviewed the access security procedures in effect for the Oracle database. We then compared the list of individuals authorized to access the Client Tracking System to the MRC official personnel list to determine whether those individuals were current employees.

To determine whether data processing assets at the MRC administrative office were adequately safeguarded, we reviewed physical security and environmental protection over the microcomputer systems through observation and interviews with MRC management and staff. To determine whether adequate controls were in place to properly account for IT-related assets at MRC offices, we initially reviewed hardware and software inventory control procedures. In addition, we tested a sample of inventory items to determine whether computer equipment located at the MRC administrative office, including microcomputers and laptop computers, were properly tagged with state identification tags, and whether the tag and serial numbers attached to the computer equipment were accurately recorded on the hardware inventory record. Subsequently, we compared computer equipment recorded on MRC's inventory record to actual equipment on hand.

To determine whether the MRC could account for all copies of application software residing on server and workstation hard drives, we first sought to obtain a current software inventory record. Because MRC was unable to provide a software inventory record, we attempted to ascertain the total number and type of software licenses MRC had by listing purchased software from the physical licenses available at MRC.

To determine whether the MRC could ensure that only authorized copies of software were installed on the automated system, we initially interviewed the MIS Director regarding procedures to install and monitor software installed on the LAN file servers, microcomputer systems, and laptop computers and obtained a current list of authorized software. We then compared the list of authorized software to software on sampled microcomputer systems.

To ascertain whether MRC was properly safeguarding and disposing of confidential client data, we interviewed management regarding confidential data and observed MRC’s confidential document

disposal process. We then assessed MRC's compliance with confidentiality and privacy laws, regulations ands MRC's policies and procedures, including compliance to retention policies.

To evaluate business continuity planning, we assessed the relative criticality of the Commission's automated systems and IT resources, determined whether the Commission had assessed system criticality and had developed documented business continuity plans for mission-critical and essential IT systems. As part of our evaluation of controls related to business continuity, we evaluated MRC's policies, procedures, and controls to ensure that adequate magnetic copies of backup media were stored in secure on-site and off-site locations, and whether successful restores of the system could be performed from stored magnetic media. In addition, to evaluate the adequacy of controls to ensure that data files and software would be available should the automated system be rendered inoperable, we interviewed department management responsible for creating backup copies of computer-related media. To assess the adequacy of business continuity planning, we reviewed the adequacy of formal planning to resume IT operations should the LAN file servers and microcomputer systems be damaged or destroyed. We also determined whether MRC's business continuity plan had been reviewed for feasibility and determined whether successful tests of the plan had been performed. We interviewed MRC management to determine whether the criticality of application systems had been assessed and whether risks and exposures to computer operations had been evaluated.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted industry auditing practices.

AUDIT SUMMARY

Based on the results of our audit, we found that internal controls in place at the Massachusetts Rehabilitation Commission (MRC) provided reasonable assurance that the IT-related equipment inventory was being safeguarded and properly accounted for and that only authorized software was residing on its computers. However, we found that certain IT-related controls needed to be implemented or strengthened regarding software inventory, business continuity planning, and logical access security administration.

Our audit revealed that adequate controls were not in place to provide reasonable assurance that software would be adequately accounted for. As a result, information with respect to the MRC's total asset value as reported to the Office of the State Comptroller on MRC's GAAP report may be incorrect. Information from GAAP reports is used to produce the Commonwealth's combined financial statement.

With respect to business continuity planning, we determined that, although backup procedures for mission-critical applications operated on the IBM mainframe were sufficient, the MRC needed to implement a formal business continuity plan to regain processing of mission-critical and essential LAN and microcomputer-based systems should the systems be rendered inoperable. Regarding access security, although the Commission had taken steps to improve logical access security, certain access security controls needed to be strengthened to provide reasonable assurance that only authorized access could be gained to automated records. In particular, controls needed to be strengthened regarding password administration and access to the test database containing information from the Client Tracking System.

Our review of internal controls indicated that the Commission had a defined organizational structure, clearly delineated reporting responsibilities, documented job descriptions, and management awareness of internal control. We found that the MRC had developed an "Internal Control Plan" to comply with Chapter 647 of the Acts of 1989.

We determined that the MRC had submitted the GAAP Report for the 2000 fiscal year to the Office of the State Comptroller. However, our audit disclosed that there were significant discrepancies between the cost figures for hardware and software listed on the inventory record and those on the GAAP report. We recommend that, in the future, MRC should reconcile GAAP report figures to the current inventory record for IT resources.

We believe that MRC should strengthen its controls over software inventory. Although adequate controls were in place to properly account for computer equipment, inventory controls needed to be strengthened to properly account for software. We found that proper internal control procedures were not in place to safeguard and properly account for software packages installed on

the LANs, the microcomputer systems, and laptop computers at Commission offices. As a result, a current, accurate, and complete software inventory record could not be provided. We believe that the MRC should develop written policies and procedures regarding software inventory controls; develop a current, accurate, complete, and valid software inventory record; document the Commission's procedures regarding the installation of software on the microcomputer systems; and periodically review the inventory record of software residing on the LANs and the microcomputer systems, and reconcile the software inventory records.

We acknowledge that MRC management and staff were aware of legal restrictions related to the use of software. Regarding authorized use of microcomputer-based software, we found that the MRC's IT Department had installed on all computers software that had been approved for use by the MRC. This installation included a new Microsoft NT operating system which is a more secure operating system than had been previously installed. Additional benefits of the installation were the simultaneous removal of any software that may not have been approved and implementation of technical restrictions for installing other software.

Our audit disclosed that logon ID and password administration for the LANs, microcomputer systems and laptop computers needed to be improved to ensure only authorized access to MRC systems. We determined that although access security software had been installed on the LAN file servers and on the microcomputer systems that might contain confidential information, not all the features of the software had been invoked. Specifically, features requiring a minimum password length and a specified frequency of password change had not been established by IT security staff. Although our tests of active user accounts indicated that only authorized users were allowed to access the system, the MRC should develop procedures to ensure that an adequate length and composition of passwords is made and that passwords are changed on a frequent basis.

Our audit revealed that the MRC had not implemented a formal, tested business continuity plan for restoring mission-critical and essential business functions in a timely manner should the automated systems be rendered inoperable or inaccessible. We determined that although the ITD-generated backup copies of transaction and master files for the Client Tracking System operated on the IBM mainframe, the MRC had not developed contingency plans to regain the functions supported by this system should the IBM mainframe be inoperable or unavailable. We believe that as the MRC implements a LAN-based case management system, a risk analysis and assessment of the LANs and microcomputer systems should be performed, and, based on the results, the Commission should develop a formal business continuity plan. The MRC should ensure that the business continuity plan is adequately tested and that procedures are established to maintain the viability of the plan. In addition, we determined that the off-site storage of computer-related media needed to be improved for mission-critical and essential data files and software for the LAN and microcomputer-based systems.

Our audit revealed that adequate controls were in place to ensure that MRC was properly securing and disposing of confidential client information that was in a hardcopy form.

AUDIT RESULTS

1. Software Inventory

Our audit determined that although MRC was using its fixed-asset inventory record to include IT resources, we found that the system of record contained computer equipment but did not identify software packages. We also determined that in the absence of maintaining software data on the fixed asset inventory, the MRC did not maintain a separate inventory list of software packages. Given that MRC's overall inventory of computer hardware at the time of our audit consisted of several file servers and approximately 1,200 on-line and laptop workstations with an estimated value of $3.28 million, the number of software packages installed could be valued at least $630,000. The lack of a software inventory record, whether included in fixed assets or as a separate inventory record, inhibits the Commission's ability to verify its reported GAAP totals for IT resources to the Office of the State Comptroller. The absence of a software inventory record also decreases the Commission's ability to determine whether only authorized software is installed on its IT infrastructure. The absence of a software inventory was noted in our prior audit report, No. 96-0054-4C, issued July 16, 1997. We recommend development of a software inventory record to properly account for and help safeguard those software products installed on the Commission's computer systems.

Sound management practices and generally accepted industry standards for IT installations advocate that a perpetual inventory be maintained for all computer equipment and software and that policies and procedures be in effect to ensure the relevance, integrity, and availability of the inventory record. In addition, prudent business practices advocate that the software inventory be used to help prevent unnecessary software expenditures, unauthorized installation of software, and software copyright infringements. Tests of software inventory against purchase records and software installed enables organizations to detect misplaced, lost, missing, unauthorized, or illegal copies of software. In accordance with the Massachusetts General Laws, each state agency is required to maintain complete and accurate records of state-owned assets and to report on the value of those state-owned assets to the Office of the State Comptroller.

Due to the lack of a software inventory record, MRC management could not properly account for all copies of software installed on its file server and on-line workstations and laptops, or determine whether only authorized software was residing on these systems or whether software had been properly allocated. In addition, the absence of a software inventory record precluded an accounting of the total number of software copies allowed under certain license agreements, and inhibited the Commission from having an accurate accounting of software inventory costs. Further, without accurate inventory costs, information submitted on the GAAP Report to the Office of the State Comptroller would have understated software valuations.

MRC management acknowledged that the Commission had purchased microcomputer workstations that had pre-loaded bundled software, but that IT resource vendors had not provided sufficient detail to separate the costs of hardware and software. At the time of our audit, the MRC did not have procedures in place to ensure that information regarding bundled software would be captured for inventory record purposes.

To assist in periodic monitoring of software packages, MRC contracted with a vendor to install Microsoft's Systems Management Server (SMS) software to enable the file servers to automatically inventory software on individual machines whenever the workstations logged onto the LAN. Although the vendor was unable to correctly install SMS, it was MRC's intention as of the end of our audit to retry the installation of SMS on Windows 2000. In addition, MRC had previously removed all software packages from every MRC workstation and laptop and replaced the deleted software with only authorized software packages. At that time, the MRC also replaced its file server-based operating system with the more secure Microsoft NT operating system.

Recommendation:

The MRC should expand the use of their fixed-asset inventory record to include software packages, system utilities, and any other software products. The Commission should develop documented policies and procedures for maintaining a software inventory. The established procedures should include identifying required data fields related to software inventory, procedures to capture information regarding bundled software, and procedures for reconciliation of the software inventory record to procurement records, software deletion, and installed software.

We further recommend that the MRC pursue the installation of Microsoft's SMS software to assist in verifying the Commission's system of record for software inventory by identifying software packages installed on MRC's IT infrastructure. We recommend that procedures be established to ensure that the GAAP Report submitted to the Office of the State Comptroller accurately and completely reflects the value of the Commission's software.

Auditee's Response:

> *Software inventory is a problem area for this agency as well as other state agencies. Our primary focus on the purchase of software is that we purchase sufficient license agreements (software or use certificates) to comply with the provider's requirements for its use. All purchasing records for our software is available at the agency and we will reconstruct a software inventory and advise the OSA upon completion. The agency has insured that only authorized software is installed on networked PC's and is reasonably assured that any additional stand alone PC's contain only authorized software. This inventory would not be included in the Comptrollers GAAP report because it falls below the cost per unit threshold requirement for GAAP reporting. This software inventory will become part of the agency internal inventory and we will develop policies and procedures to insure that this inventory is maintained.*

Auditor's Reply:

We are pleased that the MRC will establish a software inventory record. We understand that difficulties may arise in establishing and maintaining inventory records related to software. However, once established, the records should be maintainable given the use of standard software packages throughout Commission offices. We acknowledge that the MRC has taken sound steps to reduce the risk that unauthorized software would be used on the Commission's computer systems.

2. Business Continuity Planning

Our prior audit report, No. 96-0054-4C, revealed that the MRC had not implemented or tested a formal business continuity plan for a timely post-disaster restoration of mission-critical and essential business functions processed through applications residing on LAN file servers or microcomputer systems. We had found at that time that the MRC had not established contingency plans to recover and maintain business operations that were supported by ITD's IBM mainframe computer system, should that system be inoperable or unavailable. Also, the Commission had not designated or tested alternative processing sites for various Commission offices to be used should a disaster render any offices unusable or inaccessible.

Our current audit determined that the Commission did not have a written, tested business continuity plan in place to provide reasonable assurance that business functions supported by technology could be reestablished should IT systems be inoperable or unavailable. The MRC lacked a clear understanding or consensus of what steps would be followed to regain business operations for various scenarios where IT operations were lost or unavailable. Because the MRC's IT operations are distributed across the area and district offices, the loss of IT operations at one office may not have a material impact for the Commission as a whole, but may significantly impact services generated from that office. On the other hand, if ITD were unable to recover the Client Tracking System, the impact to MRC would be more adverse. Based on our understanding of ITD's backup procedures, there is a reasonable likelihood that ITD would be able to recover MRC's operations.

We found that ITD generated backup copies of data files and programs for the Client Tracking System operated on the IBM mainframe in Chelsea and that the MRC had on-site backup copies of magnetic media for their LAN-based operations. However, adequate controls were not in place to ensure that MRC-based data files would be backed up in secure off-site locations. The availability of backup copies of transaction, master files and programs would help ensure that MRC could recover its IT processing capabilities.

Given the absence of recovery plans, including designated alternative processing sites, a disaster impacting the administrative office and/or the area and district offices could seriously affect MRC's ability to regain mission-critical and essential IT-supported operations. A business continuity plan should document the MRC's recovery strategies with respect to various disaster

scenarios. Without a formal, tested recovery plan, critical and essential information related to the Commission's clients and programs, such as Vocational Rehabilitation, may be unavailable should the automated system be rendered inoperable.

The objective of business continuity planning is to help ensure the continuation of mission-critical functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted control practices and industry standards for IT operations support the need for each entity to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans, if required. To that end, the entity should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and develop its recovery plans based on the critical aspects of its information systems.

The success of the business continuity planning process requires management commitment. Senior management and system users should be closely involved in business continuity planning to help ensure that they have a clear understanding of the entity's information systems environment, determinations of systems criticality and the risks and exposures associated with the systems are correct, appropriate data processing and user area plans are developed based on the relative criticality and importance of systems, and adequate resources are available. Entities need to perform a risk analysis of the systems and clearly understand the impact of lost or reduced processing capabilities. The risk analysis should identify the relevant threats that could damage the systems, the cost of recovering the systems, and the likelihood of the threat and the frequency of occurrence.

Since MRC is migrating the Client Tracking System from the ITD's IBM mainframe to a LAN-based case-management system, it is imperative that a business continuity plan be created. Once the Client Tracking System resides solely on MRC file servers, MRC will no longer be able to rely on the ITD for backup copies of computer media essential for recovery should a disaster occur. MRC management stated that they planned to develop a business continuity plan once the Client Tracking System was migrated from the ITD's IBM mainframe to a LAN-based case management system. A business continuity plan, which is approved and tested, should be one requirement MRC sets before severing ties with the ITD with respect to the Client Tracking System and client-related data.

Recommendation:

We recommend that a risk analysis and criticality assessment be performed. Based on the results of this analysis and the identification of the relative importance of automated systems and IT resources, we recommend that MRC develop a business continuity plan that incorporates contingency plans to address various disaster scenarios. We suggest that the effort be triaged to

focus first on developing contingency plans for those operations or functions having the highest adverse impact of the loss of IT operations and on the migrated Client Tracking System. We further recommend that the plan include provisions for adequate on-site and off-site backup media copies, an alternate means of processing, and requirements for initially and periodically testing the entire plan. Once the plan has been documented, reviewed, tested, and approved, copies should be distributed to all parties who are assigned duties and responsibilities within the plan, and a copy should be stored at a secure off-site location. We recommend that the MRC evaluate their provisions for off-site storage of magnetic backup media for data files residing on MRC-managed IT systems.

Auditee's Response:

> *The Agency fully agrees with the OSA's recommendation that the agency develop a Business Continuity Plan. Disaster recovery plans, to the point that we can exercise control over, are a necessary part of the Agency EDP policy and procedures. The current critical EDP systems that allow us local and central office access to statewide systems operations (MMARS, HR/CMS, etc.) is totally dependent on the state ITD Operations. As a small State Agency, we lack the resources (dollars, personnel and technical expertise) to recover from a major systems disaster. Our planning therefore relies on the ability of the state's ITD operations for access to and safeguarding of Agency data. We do recognize that we must improve our ability to recover from a disaster to our central office server that includes our new client information system. We are taking steps to improve data backup and recovery procedures in our central office EDP operations. As a short-term solution we will locate a backup server at a remote site and test our ability to operate from that site. We will also work with ITD and other Agencies in order to develop formalized plans that will insure our operational recovery in the event of a loss of our central office or a local area office.*

Auditor's Reply:

We concur with MRC's intention to address business continuity planning. We agree with the approach of developing a plan in conjunction with ITD and to provide a means of alternative processing. The use of a file server as a means of off-site backup appears to be a good short-term strategy. Once elements of the plan are established, they should be tested and documented.

3. Logical Access Security Administration

Our audit disclosed that, although adequate logical access security had been implemented for applications operating on the ITD's IBM mainframe (such as MMARS and the MRC's Client Tracking System) and that steps had been taken by MRC to improve IT operations and security, logical access security needed to be strengthened for access to the LAN from on-line workstations and connected laptop computers. At the time of our audit, an adequate level of control had not been established at the LAN and workstation-based level since the minimum password length for system

access had not been set to require a character length greater than one and that passwords were not required to be changed at any established time periods. In addition, controls over the data used in the test database needed to be strengthened to ensure that only authorized access was granted to any electronic data.

Our audit discovered that although MRC had upgraded it's LAN and workstation operating systems to one having stronger access security features, some of those features had not been activated at the time of our audit to take full advantage of the improved controls. We found that two of the system's control features remained at a level that did not require password length to be longer than one character and that passwords be changed at predefined time periods. Although passwords of more than one character may have been used, the system was not being used to ensure that only passwords of an appropriate length be used. Generally accepted guidelines for password length indicate that passwords of less than six to eight characters not be used. Ensuring an adequate length and composition of passwords along with other controls helps to ensure that only authorized access is gained to data files and programs.

Because the access security features had not been properly implemented, logon ID and password security functions did not provide reasonable assurance at the LAN and microcomputer-based level to prevent unauthorized access to confidential client-related data files and software. As a result, confidential and/or critical data files could be placed at risk of unauthorized access, disclosure, changes or deletions. According to MRC senior management, they were unaware that the access security software on the LAN file servers and microcomputer systems had not been fully implemented.

In addition to the security features noted above, at the time of our audit, controls needed to be strengthened over confidential client data used in MRC's test database. As of the end of our fieldwork, MRC was in the process of migrating the operation of its 20-year-old Client Tracking System from a mainframe computer environment to a file server environment that used an Oracle database to provide improved functionality, access and speed. We found that the new system, known as the Massachusetts Rehabilitation Commission Information System (MRCIS), was being parallel tested using a copy of actual client data. Although the MRC's official system remained as the Client Tracking System, changes to data were being initiated in both the production and test systems. Our audit found that the level of security used over the test system was less than that used for the production system.

Although access security to the Oracle database can be implemented to use up to 14 levels of security based logon IDs and passwords, MRC's test environment did not require passwords to control access to functions, features and data within the database. Since passwords were not necessary to access the database in the test environment, access was granted solely by using a logon ID. As a result, security profile levels being used in the mainframe production environment were

not in place in the test environment. Because MRC was operating in a parallel test environment, the same level of control over data in the production environment should have been in place over the data in the test environment. Since logon IDs are known or available to all MRC staff, users of the test system for whom a password is not necessary to access the database could gain unauthorized access to certain data by using a logon ID that has a higher level of access privileges than the logon ID assigned to them. The risk here might be that individuals would be able to gain access to data files that from which they were previously restricted.

Although MRC has conducted various tests of the database, final testing of access security had not been completed at the end of our audit fieldwork. We found that database security, which relies on logon IDs and passwords, was not scheduled for password synchronization with the upgraded operating system until October 2001. As a result, the test database that contains client records could be vulnerable to unauthorized access until both logon IDs and passwords are used when the system is fully implemented.

We further noted that change controls needed to be strengthened for the Oracle-based system to ensure that relevant information is captured in appropriate audit trails to record all changes to data files. At the time of our audit, sufficient control was not in effect to ensure that MRC would know which data were changed, when, and by whom. Until the new Oracle system is fully implemented, MRC will be performing parallel data input to the IBM system as well as to the new system.

We reviewed access to the MRC's ITD-based system operated on the IBM mainframe. Based on our review of users granted access to the system to the current official MRC employee list, we determined, as of the date of our test, that only authorized users had access to the automated systems.

We acknowledge that MRC understands that, because of the nature of the data residing in the Client Tracking System, the data should be protected against unauthorized access, change, or disclosure. Massachusetts General Law Chapter 6, Section 84, states, in part, that "all records relating to clients and applicants of the commission and all personal and medical information or records given or made available to the commission, including but not limited to, names and addresses of clients and applicants, shall be confidential and for the exclusive use of the commission in the discharge of its duties. Such records or information shall not be open to the public notwithstanding the provisions of section 10 of chapter 66 or any other general or special law."

Generally accepted computer industry practices promote the implementation and use of formal control procedures for logical access security to prevent and detect unauthorized system access. The control procedures should include written policies and procedures regarding password formation; passwords should be at least eight alpha-numeric characters in length, and use and require periodic changes of passwords and formal procedures to grant authorized access and to deactivate logon IDs and passwords when an employee's status changes.

Failure to implement adequate controls regarding logical access security could result in unauthorized system access, use or modification. If unauthorized access were to be gained to the data files, there is a risk of unauthorized modifications or deletions of critical and important data or disclosure of confidential information related to the Commission's clients.

Recommendation:

We recommend that all access-security related functions of the operating systems be fully deployed, specifically to require passwords of at least eight alphanumeric characters and require that passwords be changed at least every 90 days. We also recommend that the Oracle database-related security features be synchronized with the Microsoft NT operating system before October 2001 to prevent users with IDs only from accessing the Client Tracking System. We further recommend, that once the Client Tracking System is ready to be placed in production, all client data in the legacy IBM system and the new Oracle database be reconciled and that any discrepancies be identified and resolved.

Auditee's Response:

> *We are in agreement with the OSA's recommendation that all access security related functions of the operating system be fully deployed. This access of an eight alphanumeric character password would be similar to the standard ITD requirement already in place for the MMARS, HRCMS, and other ITD supported systems and will require a change every 60 days. Due to our current implementation of our new client information system and the need to advise and train staff on these new procedures we will phase in the tighter security requirements over the next 2 months. This logon user ID and password will also apply to the SQL client database. We will also reconcile our client legacy client data to our new database during the months of October to December 2001 as part of our planned parallel operations.*

Auditor's Reply:

We are pleased that MRC will be taking action in the near future to strengthen controls over access security in accordance with our recommendations. We recommend that the MRC establish procedures to monitor and evaluate access security to determine whether existing and planned controls are working as intended. We will review process on this important issue during our next IT audit.

PRIOR AUDIT RESULTS RESOLVED

1. Inventory Control over Computer Equipment

Our prior audit determined that certain controls related to the recording and reporting of the MRC's computer equipment, valued at $2.6 million needed to be strengthened. Our current audit revealed that this issue has been resolved. During the current audit, we obtained a January 4, 2001 inventory list containing 2,952 computer-related items valued at approximately $3.28 million. Our audit confirmed that all sampled items were properly tagged with state identification numbers and that the inventory contained a corresponding inventory identification tag number, as well as cost and location of the specific items recorded. We were able to verify, on a sample basis, each of the 59 items from the inventory listing to the actual item and traced ten items back to the inventory. We also traced a sample of 32 recently-purchased items to the inventory record.

The MRC maintains a perpetual inventory record of computer equipment, and an annual physical inventory has been performed at the close of each fiscal year and subsequently reconciled to the inventory record. As a result, MRC could be assured that all hardware items purchased or acquired from surplus property were listed on the inventory record. In addition, the MRC could ensure that all hardware items transferred to the Commonwealth's Surplus Property Office in the Operational Services Division, or reported missing or stolen, were removed from the inventory record.

Although the MRC is submitting a form to the Office of the State Comptroller containing summary inventory data, we noted that MRC was not reconciling the data to the GAAP report.

Our audit disclosed that although the MRC's "Internal Control Plan" documented policies and procedures regarding the maintenance of equipment inventories and the tagging of equipment items, the plan did not include procedures for performing an annual physical inventory or reconciling the physical inventory with the perpetual inventory record. In addition, the plan did not include directives regarding compliance with the annual reporting requirements of the Office of the State Comptroller.

We recommend that the GAAP report be reconciled to the Comptroller’s inventory record form, that the MRC internal control plan require an annual physical inventory and that it reference compliance with the Office of the State Comptroller’s inventory control directives.

2. Authorized Use of Software

Our prior audit, No. 96-0054-4C issued July 16, 1997, found that the MRC needed to strengthen its internal controls to ensure that only authorized software was installed on the LANs'

file servers and microcomputer systems. The audit disclosed that although the MRC maintained a list of software packages authorized for use, the list had not been updated since 1992, and a comprehensive inventory record of software was unavailable. In addition, we found that controls had not been implemented to prevent or detect the installation or use of unauthorized or illegal copies of licensed software. Moreover, the MRC had not developed written policies and procedures regarding the authorized and appropriate use of microcomputer-based software. Further, the MRC did not implement a central repository for documentation such as licenses, manuals, or original diskettes. We determined that, at the date of our audit, MRC did not maintain an inventory record of software to keep track of software available for use.

The current follow-up audit has determined that, MRC has taken several steps since the completion of the prior audit in order to gain control over its software. MRC has recently installed on its file servers and microcomputers a more secure operating system. The new operating system allows the MRC MIS Manager the ability to prevent installation of any software that has not been approved by the MIS Department. When MRC installed the new operating system on all the microcomputers, it was done from a master disk that contained all approved software for MRC staff. This operating system installation also had the benefit of removing any unapproved software from the microcomputers.

During fiscal year 2000, in an effort to maintain a complete software inventory, MRC attempted to install Microsoft SMS software. This software would have allowed the MIS Department to inventory software on the microcomputers when the microcomputers connect to the LAN. Unfortunately, the installation was not performed correctly. As of the end of our audit, MRC was attempting to correct the problem to install SMS on a file server, which was using the current Microsoft NT operating system, by installing SMS on a just-released upgrade to the operating system.

As of the end of our audit, MRC did not have a software inventory record and planned to create one following the SMS installation. At that time, MRC would need to reconcile the compiled inventory to the listing of purchase vouchers of computer equipment and then submit the total to the Comptroller via the GAAP report.